U. S. Department of Homeland Security

United States Coast Guard

Commandant
United States Coast Guard

2703 Martin Luther King Jr Ave SE
Washington, DC 20593-7000
Staff Symbol: CG-0921
Phone: (202) 372-3500
FAX: (202) 372-2311

TESTIMONY OF
REAR ADMIRAL WAYNE R. ARGUIN
ASSISTANT COMMANDANT FOR PREVENTION POLICY

AND

REAR ADMIRAL JOHN C. VANN
COMMANDER, COAST GUARD CYBER COMMAND

ON

"PORT CYBERSECURITY: THE INSIDIOUS THREAT TO U.S. MARITIME PORTS"

BEFORE THE
HOUSE COMMITTEE ON HOMELAND SECURITY
TRANSPORTATION & MARITIME SECURITY SUBCOMMITTEE

29 FEB 2024

Introduction

Good afternoon, Chairman Gimenez, Ranking Member Thanedar, and distinguished Members of the Subcommittee. We are honored to be here today to discuss a top priority for the U.S. Coast Guard: protecting the Marine Transportation System (MTS). At all times, the U.S. Coast Guard is a military service and branch of the U.S. Armed Forces, a Federal law enforcement agency, a regulatory body, a co-Sector Risk Management Agency, a first responder, and an element of the U.S. Intelligence Community (IC). The Service is uniquely positioned to ensure the safety, security, and stewardship of the maritime domain.

Since the early days of the Revenue Cutter Service, the Service has protected our Nation's waters, harbors, and ports. While much has changed over the centuries – with our missions expanding from sea, air, and land into cyberspace – our ethos and operational doctrine remain steadfast. Regardless of the threat, we leverage the full set of our authorities; the ingenuity and leadership of our workforce; and the breadth of our military, law enforcement, and civil partnerships to protect the Nation, its waterways, and all who operate on them.

The Criticality of the Marine Transportation System

Our national security and economic prosperity are inextricably linked to a safe and efficient MTS. It is difficult to overstate the complexity of the MTS and its consequence to the Nation. It is an integrated network that consists of 25,000 miles of coastal and inland waters and rivers serving 361 ports. However, it is more than ports and waterways. It is cargo and cruise ships, passenger ferries, waterfront terminals, offshore facilities, buoys and beacons, bridges, and more. The MTS supports $5.4 trillion of economic activity each year and supports the employment of more than 30 million Americans.

It supports critical national security sealift capabilities, enabling U.S. Armed Forces to project power around the globe. The U.S. Coast Guard remains laser-focused on the safety and security of this system as an economic engine and strategic imperative.

Port Security – A Shared Responsibility and Layered Approach

The U.S. Coast Guard is the Nation's lead Federal agency for safeguarding the MTS. The Service applies a proven prevention and response framework to prevent or mitigate disruption to the MTS from the many risks it faces. U.S. Coast Guard authorities and capabilities cut across threat vectors, allowing operational commanders to quickly evaluate risks, apply resources, and lead a coordinated and effective response.

The U.S. Coast Guard works across multiple levels of government and industry to assess security vulnerabilities, determine risk, and develop mitigation strategies. This layered approach—from the local to the international level—is critical due to the size and interconnectedness of the MTS.

Locally: Vessel and Facility Security

Security in U.S. ports and waterways starts with individual vessels, port facilities, and outer continental shelf facilities. The Maritime Transportation Security Act (MTSA) and its implementing regulations place specific requirements on regulated entities to conduct security assessments, analyze the results, and incorporate their findings in U.S. Coast Guard-approved security plans.

These plans set baseline requirements that regulated U.S. vessels and facilities must follow to protect the MTS, including addressing access control, computer systems and networks, restricted area monitoring, communication, security systems, cargo handling, delivery of stores, personnel training, and drills and exercises. U.S. Coast Guard inspectors verify compliance with these plans during scheduled and unannounced inspections throughout a given year. Additionally, the Coast Guard released a proposed rulemaking leveraging the applicability of the MTSA regulations to further raise cybersecurity standards for vessels, facilities, and Outer Continental Shelf facilities.
For foreign-flagged vessels, the approach to security is very similar to that of MTSA-regulated domestic vessels. Per the International Maritime Organization's (IMO) International Ship and Port Facility Security (ISPS) Code, each foreign vessel must conduct a Ship Security Assessment that identifies: key shipboard operations that are important to protect; possible threats to key shipboard operations and likelihood of their occurrence; existing security measures and procedures; and potential weaknesses, including human factors, in security policies and procedures. This assessment then leads to the development of a Ship Security Plan, which must be approved by the ship's Flag Administration prior to a vessel being certificated as compliant with the ISPS Code. This certification is verified by the U.S. Coast Guard during regular compliance examinations when the vessel arrives in a U.S. port.

Regionally: Area Maritime Security Coordination

At the regional level, Area Maritime Security Committees (AMSC) are required by MTSA and its implementing regulations to serve an essential coordinating function during normal operations and emergency response. Comprised of government and maritime industry leaders, an AMSC serves as the primary regional body to jointly share threat information, evaluate risks, and coordinate risk

mitigation activities. As the Federal Maritime Security Coordinator (FMSC), U.S. Coast Guard Captains of the Port (COTP) direct their regional AMSC's activities.

AMSC input is vital to the development and continuous review of the Area Maritime Security (AMS) Assessment and Area Maritime Security Plan (AMSP). The AMS Assessment must include the critical MTS infrastructure and operations in the port; a threat assessment that identifies and evaluates each potential threat; consequence and vulnerability assessments; and a determination of the required security measures for the three Maritime Security levels.

These AMS assessments then lead to the collaborative development of AMSPs to ensure government and industry security measures are coordinated to deter, detect, disrupt, respond to, and recover from a threatened or actual Transportation Security Incident.

The U.S. Coast Guard COTP and AMSCs are also required by regulations to conduct or participate in an exercise once each calendar year to collectively assess the effectiveness of the AMSP in today's dynamic operating environment.

Nationally: Interagency Collaboration

The U.S. Coast Guard functions on behalf of the Department of Homeland Security as the co-Sector Risk Management Agency (SRMA) for the Maritime Transportation Subsector along with the Department of Transportation. As an SRMA, the U.S. Coast Guard is responsible for coordinating risk management efforts with the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), other Federal departments and agencies, and MTS stakeholders.

CISA is a key partner whose technical expertise supports the U.S. Coast Guard's ability to leverage our authorities and experience as the regulator and SRMA of the MTS. CISA integrates a whole-of-government response, analyzes broader immediate and long-term impacts, and facilitates information sharing across transportation sectors. Our relationship with CISA is strong and will continue to mature.

As an element of the IC, the U.S. Coast Guard possesses unique authorities, and has opportunity and capability to collect, analyze, and share information from domestic, international, and non-government stakeholders which operate throughout the MTS. This ability allows the U.S. Coast Guard to gain a collective understanding of threats and vulnerabilities facing the maritime domain, including physical security and cybersecurity.

Our enduring relationship with the Department of Defense (DoD) is also crucial to safeguarding the MTS. In many cases, DoD's ability to surge forces from domestic to allied seaports depends on the same commercial maritime infrastructure as the MTS. The relationship between the U.S. Coast Guard and DoD ensures the Nation's surge capability and lines of communication will be secure and available during times of crisis. By sharing threat intelligence, developing interoperable capabilities, and leveraging DoD's expertise, the U.S. Coast Guard enables national security sealift capabilities and jointly supports our Nation's ability to project power around the globe.

The U.S. Coast Guard also supports the Federal Emergency Management Agency (FEMA) in the Port Security Grant Program (PSGP) by providing subject matter expertise in maritime security. The PSGP is designed to support and protect critical port infrastructure from terrorism. FEMA is responsible for the administration and management of the program, which has distributed more than $3.8 billion to MTS stakeholders since the program's inception in 2002.

Internationally: International Port Security Program

U.S. Coast Guard efforts to secure the MTS also extend overseas. By leveraging international partnerships, including through the U.S. Coast Guard International Port Security (IPS) program, the U.S. Coast Guard conducts in-country foreign port assessments to assess compliance with the ISPS Code and the effectiveness of security and anti-terrorism measures in foreign ports. In addition, the IPS program conducts capacity building engagements to assist foreign ports in implementing effective anti-terrorism measures, where possible.

If the U.S. Coast Guard finds that a country's ports do not have effective security and anti-terrorism measures, the Service may impose additional security measures called Conditions of Entry (COE) on vessels arriving to the United States from those ports and may deny entry into the United States to any vessel that does not meet such conditions. Verification that a vessel took additional security measures when it was in foreign ports that lacked effective anti-terrorism measures may be required before the vessel is permitted to enter the United States.

The Growing Cyber Risks

Cyber-attacks can pose a significant threat to the economic prosperity and security of the MTS for which whole-of-government efforts are required. The MTS's complex, interconnected network of information, sensors, and infrastructure continually evolves to promote the efficient transport of goods and services around the world. The information technology and operational technology networks vital to increasing the efficiency and transparency of the MTS also create complicated interdependencies, vulnerabilities, and risks.

The size, complexity, and importance of the MTS make it an attractive cyber target. Terrorists, criminals, activists, adversary nation states and state-sponsored actors may view a significant MTS disruption as favorable to their interests. Potential malicious actors and their increasing levels of sophistication present substantial challenges to government agencies and stakeholders focused on protecting the MTS from constantly evolving cyber threats.

Cyber vulnerabilities pose a risk to the vast networks and system of the MTS. Cyber-attacks, such as ransomware attacks, can have devastating impacts on the operations of maritime critical infrastructure. A successful cyber-attack could disrupt global supply chains and impose unrecoverable losses to port operations, electronically stored information, and national economic activity. The increased use of automated systems in shipping, offshore platforms, and port and cargo facilities creates enormous efficiencies, but also introduces additional attack vectors for malicious cyber actors. Growing reliance on cyber-physical systems and technologies requires a comprehensive approach by all MTS stakeholders to manage cyber risks and ensure the safety and security of the MTS.

Last week, the President signed an Executive Order which further enables our port security efforts by explicitly addressing cyber threats. It empowers the Coast Guard to prescribe conditions and restrictions for the safety of waterfront facilities and vessels in port and includes reporting requirements for actual or threatened cyber incidents. With this authority, the Coast Guard issued a directive requiring specific cyber risk management actions for all owners or operators of cranes manufactured by companies from the People's Republic of China. Our Captains of the Port around the country are working directly with crane owners and operators to ensure compliance and further mitigate the threats posed by these cranes.

The U.S. Coast Guard's Approach

In support of the whole-of-government effort, the U.S. Coast Guard applies a proven prevention and response framework to prevent or mitigate disruption to the MTS from the many risks it faces.

Prevention

The Prevention Concept of Operations—Standards, Compliance, and Assessment—guides all prevention missions, including port security. It begins with establishing expectations in the MTS. Regulations and standards provide a set of baseline requirements and are critical to establishing effective and consistent governance regimes. With effective standards in place, vessel and facility inspectors verify systematic compliance activities to ensure the governance regime is working. This part of the system is vital in identifying and correcting potential risks before they advance further and negatively impact the MTS. Effective assessment is paramount to continuous improvement. It provides process feedback and facilitates the identification of system failures so that corrective actions can be taken to improve standards and compliance activities.

In addition to vessel and facility inspectors, the U.S. Coast Guard also has Port Security Specialists and MTS Cybersecurity Specialists in each Captain of the Port Zone. These dedicated staffs build and maintain port level security-related relationships, facilitate information sharing across industry and government, advise U.S. Coast Guard and Unified Command decision-makers, and plan security exercises.

Response

The U.S. Coast Guard has a proven, scalable response framework that can be tailored for all hazards. Whether a cyber or physical security incident, our operational commanders immediately assess the risk, consider their authorities, and deploy assets or issue operational controls to mitigate risks. Depending on the incident's size and severity, commanders set clear response priorities, request specialized resources to help mitigate risk, and notify interagency partners to help coordinate the response.

For complex responses, the U.S. Coast Guard maintains deployable teams with specialized capabilities that can support operational commanders across a spectrum of needs and domains. These teams include specially trained law enforcement teams that can bolster physical security, and pollution response teams that can address significant oil spills or hazardous material releases.

In addition, the U.S. Coast Guard has established three Cyber Protection Teams as commands under U.S. Coast Guard Cyber Command. These units assist Captains of the Port with measuring cyber risk and are poised to deploy in support of time-critical or nationally significant cyber activities.

Future Focus

Given today's dynamic operational environment, the U.S. Coast Guard is ever vigilant and on watch to identify emerging threats, evaluate associated risk, and apply authorities and capabilities to protect the MTS. While the U.S. Coast Guard has a proven prevention and response framework that has been honed over many years, the Service is dedicated to continually assessing and enhancing the way we execute both enduring and emerging missions. The U.S. Coast Guard's commitment is to continue to lead with the same level of professionalism, efficiency, and effectiveness that the public has come to expect.

Thank you for the opportunity to testify today and thank you for your continued support of the U.S. Coast Guard. We look forward to answering your questions.

Statement of

Rear Admiral Derek Trinque, United States Navy

Director of Strategic Plans, Policy, and Logistics, United States Transportation Command

Before the House Homeland Security Committee

Subcommittee on Transportation and Maritime Security

29 February 2024

Who We Are – Our Mission

U.S. Transportation Command's (USTRANSCOM) enduring purpose is to project and sustain combat power whenever and wherever our Nation chooses. As one of eleven combatant commands, our warfighting team is a diverse force, comprised of three component commands, one subordinate command, our allies, and our interagency and commercial partners—all of which constitutes the broader Joint Deployment and Distribution Enterprise (JDDE). Within the ever-changing strategic and operational landscape, our logistics and mobility enterprise continue to play an integral role in assuring our Nation's defense as well as to provide our national leadership strategic advantage. We must ensure the Joint Force can defend the Nation, take care of our people, and succeed through teamwork. To deter and win, the 2022 National Defense Strategy (NDS) directs the Future Joint Force to be lethal, resilient, sustainable, survivable, agile, and responsive.

The entire JDDE works together to move the right capabilities to the right place, at the right time. Our assigned Unified Command Plan (UCP) responsibilities are executed through three component commands (U.S. Army's Military Surface Deployment and Distribution Command, U.S. Navy's Military Sealift Command, and U.S. Air Force's Air Mobility Command), and one major subordinate command (Joint Enabling Capabilities Command [JECC]). Our key mobility mission areas include sealift, strategic seaports, air refueling, airlift, aeromedical evacuation, domestic rail, and motor and barge freight. The JDDE operates as a Total Force, harnessing the unique skills of Active Duty, Reserve, National Guard, Merchant Marine, and Civilian teammates who are vital to our ability to bolster warfighting readiness.

The Department of Defense's (DoD) ability to project military forces is inextricably linked to commercial industry. Our industry partners provide critical transportation capacity and

global networks to meet day-to-day and wartime requirements. USTRANSCOM also partners with other U.S. Government Departments and Agencies, such as the U.S. Department of State and U.S. Department of Transportation (DoT), especially the Maritime Administration (MARAD) as it operates and maintains the government-owned sealift fleet and oversees the administration of the Strategic Seaport Program. Within DoT we also interconnect with the Federal Highway, Federal Motor Carrier Safety, and Federal Railroad Administrations regarding DoD transportation requirements within CONUS, including rapid equipment movement needs from "fort to the port" on our national highway and railroad networks. In addition to DoT, we partner with the Defense Logistics Agency (DLA), the General Services Administration, and other key logistics partners who provide the funding for deployment and distribution operations as well as the Department of Homeland Security (DHS), the U.S. Coast Guard (USCG), the Transportation Security Agency, and many more. Both individually as well as collectively, this entire collective group of partners support as well as guide our efforts and are also customers of the Defense Transportation System.

With our partners, USTRANSCOM works hard to develop the most robust transportation network possible, both for current and future operations. Because our networks are vulnerable to a wide range of threats, from climate change to nation-state cyber-attacks, USTRANSCOM plans, operates, and routinely exercises so that our forces can operate through disruption. This includes operating with partners in a cyber degraded or denied environment and quickly and creatively rerouting critical supplies to support our warfighters. I will address some of our flagship efforts today.

Strategic Seaport Program

To successfully execute our deployment mission, USTRANSCOM relies on a collection of both DoD and commercially owned U.S. Strategic Seaports managed through the Strategic Seaport Program. Strategic Seaports are vital nodes in the Nation's transportation network and play a critical role in DoD's ability to deploy forces and equipment worldwide – six military seaports and eighteen U.S. commercial seaports are officially designated as primary DoD Strategic Seaports with an additional one military and thirteen U.S. commercial seaports identified as Alternate Seaports.

The basis for the program can be found in various government publications, including Executive Order 12656 regarding the assignment of emergency preparedness responsibilities. These publications direct Federal departments to identify facilities and resources, both government and private, essential to the national defense and mobilization readiness; assess the vulnerabilities and develop strategies, plans and programs to provide for the security of such facilities and resources; and to avoid or minimize disruptions of essential services during any national security emergency. The primary purpose of the Strategic Seaport Program is to ensure DoD has access to sufficient seaport capacity to meet the Nation's objectives.

Strategic Seaports

Within the UCP, USTRANSCOM is identified as the DoD Single Port Manager. The Military Surface Deployment and Distribution Command (SDDC), as the surface transportation component to USTRANSCOM, executes the Strategic Seaport Program for the DoD. Strategic Seaports are formally designated by the Commanding General, SDDC, based on anticipated deployment requirements related to plausible major contingencies, emergencies or disasters and

war. Although participation in the Strategic Seaport Program is voluntary, the Strategic Seaports accept specific planning and reporting responsibilities.

National Port Readiness Network

Once designated, the Strategic Seaports are administratively managed through the National Port Readiness Network (NPRN). The NPRN is made up of nine government agencies including USTRANSCOM, SDDC, Military Sealift Command (MSC), U.S. Northern Command, U.S. Forces Command, U.S. Coast Guard (USCG), U.S. Army Corps of Engineers, Transportation Security Agency, and MARAD who Chairs the NPRN. The NPRN provides coordination and cooperation to support the safe and secure movement of military forces through the Strategic Seaports. A Memorandum of Understanding (MOU) outlines each of the nine agencies' roles, responsibilities, and authorities to facilitate planning and support port readiness.

Port Readiness Plans

Each designated primary Strategic Seaport has a Port Readiness Plan (PRP) which identifies the specific port facilities and berths that would be made available to DoD within forty-eight hours of issuance of a rated order contract. These port facilities include berths, open and covered staging areas, rail spurs, and marshaling yards which can readily accommodate the trans-load of substantial numbers of DoD's rolling stock and containers within anticipated short timelines. MARAD serves as the primary interface with the commercial Strategic Seaports to establish and maintain the PRPs.

Port Readiness Committees

Chaired by the USCG Captain of the Port (COTP), the Port Readiness Committee (PRC) is convened biennially to facilitate training and periodic exercises to ensure the readiness of the

port to support military operations. The PRC is comprised of local port or port area representatives that coordinate, evaluate, and test military out load plans, force protection/ military out load security and facilitate out loads.

Readiness Reporting

The Strategic Seaports formally report to MARAD quarterly on their ability to make PRP facilities available to support DoD's needs. Informal, off-cycle reporting is also completed as events warrant. Additionally, MARAD conducts an annual Enhanced Port Readiness Assessment on each Strategic Port, with the assistance of the other members, to ensure the PRC has a current understanding of the port's ability to support military operations. These assessments cover the availability of facilities and labor, port access, port security, and other factors that may interfere with deployment.

Ports for National Defense Program

The Director of SDDC's Transportation Engineering Agency is designated as the Special Assistant for Transportation Engineering to provide executive-level representation for DoD on all transportation engineering matters related to the National Defense Programs (Ports, Highways, Railroads). These programs ensure DoD can readily access and utilize the Nation's civil sector infrastructure to support major force deployments by assessing and monitoring the sufficiency and viability of all elements of the related infrastructure. The Ports for National Defense Program (PND) provides the engineering / analytical foundation for the DoD Strategic Seaport Program pursuant to Executive Order 12656 and in accordance with the authority in the Defense Production Act of 1950 (50 U.S.C. Section 4502, et seq.) by managing the identification and assessments of Strategic Seaports.

The PND Office views Strategic Seaport capacities from an aggregated coastal perspective (East, Gulf, West, Alaskan), and in the Pacific. Each coast currently has the aggregate capacity necessary to respond to plausible deployment requirements while also accounting for normal delays (e.g., weather, transportation, etc.) and the potential loss of one or more Strategic Seaports to manmade events or natural disasters. The criteria PND uses to support the designation of a Strategic Seaport extends beyond port infrastructure and throughput capability. Proximity to origins (primarily Army Power Projection Platforms) and the capabilities of the transportation networks connecting these origins to the ports are also considered.

Port Look Studies

Beginning in 2008 with the publication of the original "Port Look Study," DoD has completed multiple reviews/assessments of the sufficiency of the Strategic Seaports in meeting DoD needs. Many of these reviews/assessments were congressionally directed via National Defense Authorization Act (NDAA) language or were the result of Government Accountability Office audit recommendations; however, some were self-imposed in keeping with the tenets of the Strategic Seaport Program.

To evaluate physical conditions at the Strategic Seaports, the PND Office completed the "Assessment and Report on Strategic Seaports" as directed by Section 3515 of the 2020 NDAA (Public Law 116-92). USTRANSCOM submitted this report to Congress in July 2020. This study found that while many of the ports assessed were found to have varying degrees of structural deficiencies associated with PRP facilities, none of these deficiencies were assessed to have significant impacts on near-term deployment operations.

The PND Office also recently completed the "Port Look 2021" study. This study assessed throughput capabilities at current Strategic and Alternate Seaports, accounted for threats that could have an impact on deployment operations (including cyber), assessed sufficiency of existing Strategic Seaports to meet expected deployment requirements and made recommendations to address capability gaps. The Port Look 2021 study recommended the designation of an additional Strategic Seaport on the U.S. West Coast to ensure the Strategic Seaports on that coast can overcome normal delays and the loss of a port due to manmade events or natural disasters. In response to that recommendation, the commercial Port of Everett, Washington, was formally designated a Strategic Seaport in September 2021.

Interagency Security of the Strategic Seaports

While the Coast Guard is designated by the Secretary of Homeland Security as the lead DHS agency for maritime security, seaport security is a shared responsibility among private ownership, civil authorities, DoD, and other federal agencies. For example, owners, operators, masters, and agents of vessels or owners and/or operators of waterfront facilities have the primary responsibility for the protection of their vessels or waterfront facilities. Military unit commanders are responsible for the physical security of all equipment and resources under their command. Federal, state and local law enforcement agencies provide civil support, to include preventing the escalation of lawful protest activity and ensuring continuity of port operations when operations are potentially threatened by labor actions or other forms of civil disturbance

USCG and the Department of Homeland Security have overall responsibility and enforcement authority for the safety, protection and security of vessels, harbors, waterfront facilities, and maritime critical infrastructures and key resources that are carried out by the

USCG Captain of the Port. As mentioned earlier, the COTP is the chair of respective NPRN PRCs, and assists in further coordinating interagency efforts regarding port readiness issues.

TheNavy (delegated to the Naval Component Commanders) is responsible for force protection of military sealift assets. MSC, the naval component to USTRANSCOM, its Area Commands, and/or the local MSC Office coordinates for appropriate security support at commercial ports with the USCG COTP and the SDDC Brigade/Battalion Commander.

SDDC Transportation Brigade/Battalion security personnel coordinate with the appropriate port security/law enforcement authority where DoD operations are being conducted. SDDC conducts threat assessments based on Force Protection Conditions, Maritime Security (MARSEC) level, applicable National Terrorism Advisory System alerts and available intelligence and will coordinate with the COTP and Port Support Activity to ensure appropriate balanced landside and waterside safety and security measures around deployment activities.

Mission Impacts – Resiliency

In general, if Strategic Seaports fail to maintain viability and availability of the facilities outlined in their PRPs, the DoD could exercise several options to support deployment and the DoD response to national emergencies. Such options include increasing or changing PRP facilities at existing Strategic Seaports, for example negotiating for more or different marshalling areas, number of berths, staging area locations/square footage, etc. DoD could also consider designating different or additional Strategic Seaports. Finally, as previously explained, the Strategic Seaport Program is intentionally designed to carry excess capacity to mitigate lost seaport access due to exogenous events.

Mission Assurance and Risk Management

The Secretary of Defense's recently issued "Homeland Defense Policy Guidance 2023" which supports implementation of the 2022 National Defense Strategy's highest priority, defending the homeland, paced to the growing multi-domain threat posed by China.

Consistent with the Homeland Defense Policy Guidance, USTRANSCOM manages risk to Defense Critical Infrastructure (DCI) through the Mission Assurance (MA) Construct which is a process to protect or ensure the continued function and resilience of capabilities and assets, including personnel, equipment, facilities, networks, information and information systems, infrastructure, and supply chains, critical to the execution of DoD mission-essential functions in any operating environment or condition. Central to this construct is the Secretary of Defense's signed Mission Assurance Strategy with the message that in today's global risk environment, strategic planning for core defense missions must account for a wide variety of manmade and naturally occurring threats and hazards and their resultant vulnerabilities. The Mission Assurance Strategy provides the Department with a Mission Assurance-centric framework focused on ensuring resiliency for the capabilities and assets supporting our core missions.

The MA Construct outlines the process to identify the most important capabilities and assets needed for the Department to carry out its missions. These capabilities face multiple threats such as natural disasters, foreign intelligence collection, and kinetic and cyber threats. To successfully address these threats and hazards requires the collective expertise, responsibilities, and authorities from multiple organizations within the DoD and external to the DoD.

Through the MA Construct, we work across DoD to identify, analyze, assess, and monitor DCI strategic-level risks to global mobility operations and mission execution. This strategic level of risk management effort addresses the protection and resiliency of DCI

identified as critical to Operation Plan execution. Commercial, privately owned and operated infrastructure, and non-DoD publicly owned infrastructure are considered DCI to include seaports if they support a DoD mission.

Conclusion

In conclusion, Strategic Seaports are vital nodes in the Nation's transportation network and play a critical role in DoD's ability to deploy forces and equipment worldwide. We have designated eighteen Commercial Strategic Seaports and six Military Strategic Seaports, thirteen alternate commercial seaports and one alternate military seaport. Each designated Strategic Seaport has a mutually agreed upon Port Readiness Plan (PRP) which identifies both DoD's and the port's needs, expectations, and timeline requirements. Although participation in the Strategic Seaport Program is voluntary, each designated Strategic Seaports accepts specific planning and reporting responsibilities.

The coordination between USTRANSCOM and the Department of Homeland Security and the U.S. Coast Guard concerning the security of Strategic Seaports is multi-fold. Such coordination includes roles and responsibilities as identified within the NPRN nine-member interagency MOU. Each designated Strategic Seaport has an established Port Readiness Committee which is chaired by the USCG Captain of the Port. The committee is comprised of local port or port area representatives (both civilian and military) that coordinate, evaluate, and test military out load plans, force protection/ military out load security and facilitate out loads. Through the Mission Assurance Construct, USTRANSCOM also synchronizes inputs and coordinates discussions across USTRANSCOM staff directorates, component commands, DoT, DHS, as well as other relevant mission partners to include Federal Law Enforcement and Counterintelligence Communities directly supporting commercial ports.

To ensure the Joint Force's ability to deploy via our seaports, our Ports for National Defense Office has rigorously reviewed, analyzed, and compared DoD's requirements to port locations, viabilities, and capabilities. The Strategic Seaport Program is intentionally designed to carry excess capacity in order to mitigate potential lost seaport access. Each U.S. coast has the aggregate capacity necessary to respond to deployment requirements while also accounting for normal delays (e.g., weather, transportation, etc.) and the potential loss of one or more Strategic Seaports to manmade events or natural disasters.

All in all, to remain successful, USTRANSCOM must be ready to project power today and tomorrow, and we will only achieve this together. The contested nature of logistics highlights that our actions to improve mobility capabilities and to modernize the JDDE, must continue in order for the DoD to maintain advantages and deliver on our national security requirements.

Powered by dedicated men and women, USTRANSCOM underwrites the lethality of the Joint Force, advances American interests around the globe, provides our nation's leaders with strategic flexibility, and creates multiple dilemmas for our adversaries. I thank Congress for your continued support to the men, women, and mission of USTRANSCOM.

TESTIMONY OF

Christa Brzozowski
Acting Assistant Secretary for Trade and Economic Security
Office of Strategy, Policy, and Plans
U.S. Department of Homeland Security

For a Hearing

BEFORE

United States House of Representatives
Committee on Homeland Security
Transportation and Maritime Security Subcommittee

ON

"Port Cybersecurity: The Insidious Threat to U.S. Maritime Ports"

February 29, 2024
Washington, DC

Introduction:

Good morning, Chairman Gimenez, Ranking Member Thanedar, and distinguished Members of the Subcommittee. Thank you for the opportunity to appear before you today to discuss the U.S Department of Homeland Security's (DHS or Department) role in securing maritime infrastructure and bolstering supply chain resilience against potential threats posed by the People's Republic of China (PRC).

The Department is deeply committed to its national and economic security missions. Across DHS, we work diligently to address all hazards that threaten our transportation systems, critical infrastructure, and the safe and lawful flow of goods and people. The dedicated men and women of the Department work every day to protect our ports, screen and vet goods and travelers, and help infrastructure owners and operators respond to the threats of today and prepare for the threats of tomorrow. DHS leverages the extensive authorities, data, and expertise from its operational Components in trade and travel facilities, physical and cyber security, and disaster response and preparedness to protect our vital trade infrastructure, ensure the safe and lawful flow of critical goods, and protect U.S. economic security.

Supply Chain Resilience Center:

Understanding the depth and breadth of the Department's expertise, authorities, and capabilities in the economic security realm, Secretary Mayorkas has challenged the Department to coordinate and enhance its supply chain resilience efforts. In 2022, the Secretary called upon the Homeland Security Advisory Council (HSAC) to recommend new ways that DHS can advance supply chain resilience leveraging the Department's expertise and authorities. On November 27, 2023, in response to a resulting HSAC recommendation, President Biden and Secretary Mayorkas announced the creation of the Supply Chain Resilience Center (SCRC or Center) within the Office of Strategy, Policy, and Plans, to enhance coordination of the Department's supply chain efforts.

To prepare for the next economic disruption, be it a pandemic, conflict, or adversary-led market distorting activity, DHS, through the SCRC, is identifying threats to supply chain resilience, addressing security vulnerabilities, and helping Americans prepare for and mitigate supply chain disruptions. To accomplish these goals, the SCRC is coordinating all the tools at the Department's disposal, including our wide range of Component authorities and capabilities, to bolster critical supply chain resilience. By placing the SCRC within the DHS Office of Strategy, Policy, and Plans, the aim is to ensure that our many efforts to advance supply chain resilience across the DHS enterprise are more than the sum of their parts. The SCRC will ensure that the DHS approach to supply chain resilience is holistic in scope and tightly coordinated with the private sector to co-develop practical mitigations that protect our economy.

As the Department's central supply chain coordinator, the SCRC will leverage data and intelligence resources to identify future threats to critical U.S. supply chain. In this vein, we are building a Watch Center concept that will use both publicly available information and government information feeds to provide early identification of emerging or ongoing threats. The current Watch Center provides daily situational briefs to my office's leadership that

synthesizes internal and external information sources. Concurrently, we are working closely with the Department's Office of Intelligence and Analysis and the broader U.S. Intelligence Community to ensure our leaders are up to date on the latest threats.

The SCRC is collaborating closely with our interagency partners to build supply chain resilience in critical infrastructure, to ensure our nation is better prepared for and able to respond to any threat. The SCRC will seek to advance a coordinated Department of Defense-DHS approach to civilian/military supply chain resilience preparedness policy under the National Defense Industrial Strategy's implementation plan. The SCRC is collaborating with the White House and the rest of the Federal Government in the President's Council on Supply Chain Resilience to ensure a whole-of-government response to promote supply chain resilience and protect key systems and infrastructure.

To build our network of allies, the SCRC has begun establishing partnerships with foreign governments. We are working with trusted international governments to develop best practices, identify supply chain risks and shared mitigations, and coordinate exercises to test our capabilities. I am pleased to share that the SCRC will be working with other Executive Branch agencies to partner with our colleagues in Canada to assess port security processes as they relate to supply chains. Together we will conduct a binational interagency tabletop exercise later this year. The exercise will involve a simulated northern border land port disruption of trade and transportation. The exercise will address potential bottlenecks at the U.S.-Canada border and identify best practices to mitigate risks and create a more resilient border.

SCRC & Maritime Infrastructure:

Just weeks after announcing the SCRC, Secretary Mayorkas hosted a roundtable meeting with senior business leaders to introduce the SCRC and how it is leveraging DHS capabilities to identify and mitigate risks with the potential to create major supply chain disruptions. Among the topics raised were the risks posed by PRC-manufactured ship-to-shore cranes.

To better understand and test DHS capabilities to respond to threats to port infrastructure, the SCRC held its inaugural tabletop exercise to understand how the Department might respond to a supply chain disruption caused by a port cyber incident affecting ship-to-shore crane operability. Participants included members from the U.S. Coast Guard (USCG), Cybersecurity and Infrastructure Security Agency (CISA), U.S. Customs and Border Protection (CBP), Federal Emergency Management Agency (FEMA), Transportation Security Administration (TSA), and U.S. Immigration and Customs Enforcement (ICE). The exercise identified key communication areas that are well implemented, but also highlighted the need for holistic coordination planning across the Department. Our next action will be an after-action review that will provide analysis and recommendations informed by the exercise. Moving forward, we are also working to research and map key U.S. maritime infrastructure for homeland security equities. This comprehensive analysis will combine trade import data, DHS critical infrastructure information, and DHS and interagency geospatial data, and will help us to understand the landscape of U.S. maritime infrastructure security.

Concurrently, the SCRC is evaluating the risks to U.S. ports posed by adversarial nation state threats and the potential overreliance on untrustworthy equipment and vendors that are subject to nation-state control and may pose data exploitation, insider threat, and unvetted virtual and physical access risks. The SCRC is closely collaborating with port authorities and operators, other industry stakeholders, and the interagency to conduct this analysis. With this analysis, the SCRC has worked closely with USCG and CISA to verify that our authorities and capabilities are current to keep pace with this emerging threat.

Finally, the SCRC is pleased to expand upon the messages promulgated by President Biden and Secretary Mayorkas in the recent release of the Executive Order on *Amending Regulations Relating to the Safeguarding of Vessels, Harbors, Ports, and Waterfront Facilities of the United States*, USCG's Maritime Security Directive on cyber risk management actions for PRC-manufactured cranes, USCG's Notice of Proposed Rulemaking on Cybersecurity in the Maritime Transportation System, and the Administration's announcement that PACECO Corp., a subsidiary of Japanese conglomerate Mitsui, is planning to onshore crane production. To amplify these announcements, the SCRC hosted a private sector roundtable with USCG and the Office of Intelligence and Analysis to discuss the threat landscape, highlight the Executive Order's impact on port security, and gather more information from industry representatives about concerns they have.

Foreign Investment Screening:

The United States remains vigilant against the threats to the security of our nation's critical infrastructure that may arise from foreign investments such as investments in our trade and logistics sector, including our maritime ports. In addition to the SCRC's efforts, DHS has played a leading role for the past two decades on the Committee on Foreign Investment in the United States (CFIUS) by identifying and mitigating risks arising from foreign investments in port infrastructure and protecting sensitive trade and logistics data from aggregation and exploitation by foreign adversaries. By law, CFIUS analyzes the facts and circumstances of each foreign investment in port infrastructure within its jurisdiction on a case-by-case basis, following a rigorous risk-based review process. In recent years, DHS has increasingly used its role in CFIUS to lead Committee reviews and mitigation efforts related to foreign investments in U.S. container terminals, and DHS will continue to identify and mitigate other investments in U.S. maritime physical infrastructure that pose national security risks.

Through CFIUS, DHS is also moving to address new and emerging risks in the maritime space. Beyond ports, PRC investments in the global shipping and logistics supply chain permit Beijing to aggregate sensitive supply chain data, which can be exploited to target supply chain vulnerabilities, circumvent U.S. customs, export control, and forced labor laws, and monitor U.S. military logistics. As the U.S.-China Economic and Security Review Commission noted in its 2022 issue brief, *LOGINK: Risks from China's Promotion of a Global Logistics Management Platform*, China aims to monitor and shape the movement of goods around the world, including by accruing dominant market positions in shipping. The PRC increasingly seeks to collect data in foreign markets related to the shipment of goods, exemplified by the PRC Ministry of Transportation's promotion of LOGINK, a unified logistics platform to pool logistics and shipment tracking data. PRC equity investments in freight forwarders, non-vessel operating

common carriers (NVOCCs), and other third-party logistics firms may permit Beijing to aggregate and exploit trade and logistics data. DHS will use the full range of authorities available, including CFIUS, to identify national security risk, take appropriate measures such as mitigation, and – where necessary – recommend divestment to the President to protect national security.

DHS Component Efforts to Protect Maritime Ports:

The Department leverages its wide range of expertise and authorities to protect key transportation infrastructure and advance the resilience of the U.S. supply chain. In addition to USCG, which serves as the co-Sector Risk Management Agency (SRMA) for the maritime subsector and regulator for covered maritime facilities and vessels, other DHS operational Components work diligently every day to facilitate the safe and lawful flow of goods and people upon which our economic security relies.

CBP secures ports of entry throughout the United States, facilitating the lawful flow of people and goods across our borders, and deterring threats from bad actors. CBP has led the way in securing our trade infrastructure with innovative initiatives like the Customs Trade Partnership Against Terrorism. CBP has tailored this program for the maritime port community, developing security standards for marine port authority and terminal operators. CBP leverages a wide range of trade data to target high-risk cargo, enforce our nation's trade laws, protect key infrastructure, and promote supply chain resilience.

TSA plays a key role in securing our nation's transportation systems, including aspects of maritime ports, through enrollment, vetting, and credentialing programs. In partnership with USCG, TSA administers the Transportation Worker Identification Credential (TWIC), which screens workers who access the most secure areas of our maritime ports. Through the TWIC, TSA vets millions of transportation workers including longshoremen, truck drivers, and merchant mariners.

CISA works to manage and reduce risk to our nation's critical infrastructure. CISA takes a unique approach to this mission, partnering closely with critical infrastructure owners and operators and other government agencies to assess risk across the country. CISA works collaboratively with USCG, TSA, other SRMAs, and public and private sector partners to develop risk mitigation solutions for critical infrastructure organizations of all sizes. Port owners and operators can consult a range of CISA cyber and physical security guides and even request one-on-one guidance from CISA through its cadre of local and regional security advisors.

FEMA supports port owners and operators through the Port Security Grant Program in partnership with USCG. This program offers vital funding to protect ports from adversaries, enhance security risk management, improve maritime domain awareness, and implement maritime security mitigation protocols that can help ports prepare for and respond to a range of hazards.

Conclusion:

The Department is dedicated to preparing for, responding to, and mitigating any and all threats to U.S. supply chains. We are deeply committed to our national and economic security missions and ensuring all stakeholders are prepared for the threats of tomorrow. I appreciate this opportunity to testify on this issue, and I look forward to answering your questions.